On compact wavelet matrices of rank m and of order and degree N

L. Ephremidze and E. Lagvilava

Abstract. A new parametrization (one-to-one onto map) of compact wavelet matrices of rank m and of order and degree N is proposed in terms of coordinates in the Euclidian space $\mathbb{C}^{(m-1)N}$. The developed method depends on Wiener-Hopf factorization of corresponding unitary matrix functions and allows to construct compact wavelet matrices efficiently. Some applications of the proposed method are discussed.

1. INTRODUCTION

Let $\mathbb{C}$ be the set of complex numbers, and let $\mathbb{F} \subset \mathbb{C}$ be a subfield invariant under the complex conjugation. A formally infinite matrix $\mathcal{A}$ with m rows

(1)
$$
\mathcal{A} = \begin{pmatrix} \cdots & a^0_{-1} & a^0_0 & a^0_1 & a^0_2 & \cdots \\ \cdots & a^1_{-1} & a^1_0 & a^1_1 & a^1_2 & \cdots \\ & \vdots & \vdots & & & \\ \cdots & a^{m-1}_{-1} & a^{m-1}_0 & a^{m-1}_1 & a^{m-1}_2 & \cdots \end{pmatrix}, \quad a^i_j \in \mathbb{F},
$$

is called a *wavelet matrix* (of rank m) if its rows satisfy the so called *shifted orthogonality condition*:

(2)
$$
\sum_{k=-\infty}^{\infty} a^i_{k+mj} \, \overline{a^r_{k+ms}} = \delta_{ir}\delta_{js}
$$

(δ stands for the Kronecker delta). Such matrices are a generalization of ordinary $m \times m$ unitary matrices and they play the crucial role in the theory of wavelets [7] and multirate filter banks [8]. The reason for us to work with $\mathbb{F}$ instead of just $\mathbb{C}$ is that it will allow more flexibility in applications, since the proposed proofs and discussions apply to a whole range of fields including the set of real numbers, rational numbers, as well as algebraic extensions of rational numbers. A reader not concerned with general fields may assume that $\mathbb{F} = \mathbb{C}$.

In the *polyphase representation* of matrix $\mathcal{A}$,

(3)
$$
\mathbf{A}(z) = \sum_{k=-\infty}^{\infty} A_k z^k,
$$

where $\mathcal{A} = (\cdots, A_{-1}, A_0, A_1, A_2, \cdots)$ is the partition of $\mathcal{A}$ into block $m \times m$ matrices $A_k = (a^i_{km+j})$, $0 \le i, j \le m-1$, the condition (2) is equivalent to

(4)
$$
\mathbf{A}(z)\widetilde{\mathbf{A}}(z) = I_m,
$$

where $\widetilde{\mathbf{A}}(z) = \sum_{k=-\infty}^{\infty} A_k^* z^{-k}$ is the *adjoint* to $\mathbf{A}(z)$ ($A^* := \overline{A}^T$ is the Hermitian conjugate and I_m stands for the $m \times m$ unit matrix). This is easy to see as (2) can be written in the block matrix form $\sum_{k=-\infty}^{\infty} A_k A_{l-k}^* = \delta_{l0} I_m$.

Our notion of a wavelet matrix is weaker than usual. So, as the orthogonal basis of $L^2(\mathbb{R})$ can be developed (see [7, Ch-s 4, 5]), also the *linear condition* $\mathbf{A}(1)\,\mathbf{1} = \sqrt{m}\,e_1$, where $\mathbf{1} = (1, 1, \dots, 1)^T$ and $e_1 = (1, 0, \dots, 0)$, must be satisfied. In our consideration, the linear condition is irrelevant. Instead, we require the condition

$$(5) \qquad\qquad \mathbf{A}(1) = I_m$$

which much simplifies the whole exposition. For any wavelet matrix $\mathcal{A}$, $\mathbf{A}(1) = \sum_{k=-\infty}^{\infty} A_k$ is unitary (see (4)), so that the conditions (2) and (5) will be satisfied for $\mathcal{A}_0 = \left(\mathbf{A}(1)\right)^{-1}\mathcal{A}$. Note also that for any wavelet matrix $\mathcal{A}_0$ satisfying (5) and any unitary matrix U, the matrix $\mathcal{A} = U\mathcal{A}_0$ is also a wavelet matrix satisfying $\mathbf{A}(1) = U$. Thus the additional restriction (5) does not lose generality in the description of wavelet matrices. Observe that the polyphase representation of $U\mathcal{A}$ is $\sum_{k=-\infty}^{\infty} U A_k z^k$ (obviously, there is one-to-one correspondence between the matrices (1) and their polyphase representations (3) and they are naturally identified).

We consider the compact wavelet matrices, which means that only a finite number of coefficients in (1) are non-zero (the corresponding wavelet functions in $L^2(\mathbb{R})$ have then a compact support, and the corresponding filters in signal processing applications are physically realizable). Namely, compact wavelet matrices with polyphase representation

$$(6) \qquad\qquad \mathbf{A}(z) = \sum_{k=0}^{N} A_k z^k,$$

where $A_N \neq 0$, are called of (*rank m* and) *order* $N := \mathrm{ord}(\mathcal{A})$ (in some works they are called of *genus $N+1$*); we write $\mathcal{A} \in \mathcal{WM}(m, N, \mathbb{F})$. The property (4) for the matrix polynomial (6) means that $\mathbf{A}(z)$ is a *paraunitary* matrix function. Note that, in this case, $\mathbf{A}(z)$ is usual unitary matrix for each $z \in \mathbb{T} := \{z \in \mathbb{C} : |z| = 1\}$.

As the determinant of $\mathbf{A}(z) \in \mathcal{WM}(m, N, \mathbb{F})$ is always monomial, i.e., $\det \mathbf{A}(z) = c\,z^d$ (since $\det \mathbf{A}(z) \det \widetilde{\mathbf{A}}(z) = 1$), the positive integer d is defined to be the *degree* of $\mathcal{A}$, $d = \deg(\mathcal{A})$. The set of wavelet matrices of rank m, order N and degree d will be denoted by $\mathcal{WM}(m, N, d, \mathbb{F})$. It can be proved that $\deg(\mathcal{A}) \geq \mathrm{ord}(\mathcal{A})$ for any $\mathcal{A} \in \mathcal{WM}(m, N, \mathbb{F})$ and $\deg(\mathcal{A}) = \mathrm{ord}(\mathcal{A})$ if and only if $\mathrm{rank}(A_0) = m - 1$ (see Lemma 1 below). As $A_0 A_N^* = \mathbf{0}$ for each $\mathcal{A} \in \mathcal{WM}(m, N, \mathbb{F})$ (since it is the Nth matrix coefficient of the product in (4)) and $A_N \neq \mathbf{0}$, we have $\mathrm{rank}(A_0) < m$. Thus $\deg(\mathcal{A}) = N$ whenever A_0 has a maximal possible rank and it is assumed to be the nonsingular case. Throughout the paper, we will intensively study $\mathcal{WM}(m, N, N, \mathbb{F})$.

Obviously, if we shift rows of $\mathcal{A} \in \mathcal{WM}(m, N, N, \mathbb{F})$ by arbitrary multiples of m, then the obtained $\mathcal{A}_1$ is a wavelet matrix as well. However, if we make these movements chaotically, then in general $\deg(\mathcal{A}_1)$ does not coincide with $\mathrm{ord}(\mathcal{A}_1)$ and $\mathcal{A}_1$ becomes singular.

As $\mathcal{A}$ and $U\mathcal{A}$, where U is nonsingular, have the same rank, order and degree, we will additionally assume that $\mathcal{A} \in \mathcal{WM}(m, N, N, \mathbb{F})$ satisfies (5) and the subset of

such compact wavelet matrices will be denoted by $\mathcal{WM}_0(m, N, N, \mathbb{F})$. As has been mentioned above, the linear condition (5) does not lose generality in the description of $\mathcal{WM}(m, N, N, \mathbb{F})$.

Matrix polynomials $\mathbf{V}(z) \in \mathcal{WM}_0(m, 1, 1, \mathbb{F})$ are called *primitive* wavelet matrices and they always have the form $\mathbf{V}(z) = Q + Pz$, where P and Q are *complementary* (*orthogonal*) *projections* on $\mathbb{F}^m$ and $\mathrm{rank}(P) = 1 \Leftrightarrow \mathrm{rank}(Q) = m - 1$ (see [6, Th. 3.1] or Lemma 2).

Every $\mathbf{A}(z) \in \mathcal{WM}_0(m, N, N, \mathbb{F})$ can be uniquely factorized as (see [7, Theorem 4.4.15] or Theorem 2)

$$(7) \qquad \mathbf{A}(z) = \prod_{j=1}^{N} \mathbf{V}_j(z) = \prod_{j=1}^{N} \left(Q_j + P_j z\right), \quad \mathbf{V}_j(z) \in \mathcal{WM}_0(m, 1, 1, \mathbb{F}),$$

where no consecutive operators P_j are orthogonal to each other, $P_j P_{j+1} \neq 0$. This factorization gives rise to the map (parametrization)

$$(8) \qquad \underbrace{\mathbb{F}\mathrm{P}^{m-1} \times \mathbb{F}\mathrm{P}^{m-1} \times \ldots \times \mathbb{F}\mathrm{P}^{m-1}}_{N} \supset \mathcal{B} \longleftrightarrow \mathcal{WM}_0(m, N, N, \mathbb{F}),$$

where $\mathbb{F}\mathrm{P}^{m-1}$ is the projective space $\mathbb{F}^m/(\mathbb{F}\backslash\{0\})$ (the space of one-dimensional subspaces of $\mathbb{F}^m$) which is one-to-one and onto but defined only on the subset $\mathcal{B}$ where consecutive directions are not orthogonal, i.e. some singular points are excluded from the set of parameters. Until now it has been the only known simple way of constructing $\mathcal{A} \in \mathcal{WM}_0(m, N, N, \mathbb{F})$ for arbitrary N: choosing nonzero column vectors $v_j \in \mathbb{F}^m$, $j = 1, 2, \ldots, N$, such that $v_j \not\perp v_{j+1}$, taking the corresponding projections $P_j = v_j(v_j^* v_j)^{-1} v_j^*$ and primitive wavelet matrices $\mathbf{V}_j = I_m - P_j + P_j z$, and constructing the product (7) that belongs to $\mathcal{WM}_0(m, N, N, \mathbb{F})$.

REMARK 1. *The representation* (7) *resembles the factorization for ordinary polynomials* $p(z) = \prod_{k=1}^{N}(z - z_k)$ *by using their roots. However the following remarkable fact should be emphasized: to find the roots of* $p(z)$ *we have to go, in general, to a larger field than the field of coefficients of* $p(z)$. *For the factorization in* (7), *the coefficients of each factor* $\mathbf{V}_j$ *belong to the same field* $\mathbb{F}$.

Now we turn to our contribution in the study of compact wavelet matrices. This approach has been developed during a search for a new matrix spectral factorization algorithm [5], and it makes possible to parameterize $\mathcal{WM}(m, N, N, \mathbb{F})$ directly in terms of points in $\mathbb{F}^{(m-1)N}$. Moreover, compact wavelet matrices can be constructed in a more efficient way than by taking the products (7). Other advantages and possible applications of the proposed method are mentioned in the course of discussions below.

Recall that we identify $\mathcal{A} \in \mathcal{WM}(m, N, N, \mathbb{F})$ with its polyphase representation (6). The linear condition we have introduced is (5) and such a subclass is denoted by $\mathcal{WM}_0(m, N, N, \mathbb{F})$. We further require that the last row of A_N be not the zero vector and denote such a subclass by $\mathcal{WM}_1(m, N, N, \mathbb{F})$. This is done without loss of generality as $A_N \neq 0$ and we can interchange the rows of $\mathcal{A}$, if necessary. In particular, for any $\mathcal{A} \in \mathcal{WM}(m, N, N, \mathbb{F})$ there exist constant unitary $m \times m$ matrices U_0 and U_1 such that $U_0 \mathcal{A} U_1 \in \mathcal{WM}_1(m, N, N, \mathbb{F})$ (by right multiplication we assume that

$\mathcal{A}U_1 = (A_0U_1, A_1U_1, \ldots, A_NU_1)$, i.e. the polyphase matrix of $\mathcal{A}U_1$ is $\mathbf{A}(z)U_1$). Indeed, we can interchange the rows of $\mathcal{A}$, if necessary, by multiplication by U_0 and then take $U_1 = (U_0\mathbf{A}(1))^{-1}$. Hence, in what follows, we parameterize $\mathcal{W}\mathcal{M}_1(m, N, N, \mathbb{F})$.

Let $\mathcal{P}_N^+[\mathbb{F}] := \left\{\sum_{k=0}^N c_k z^k : c_0, c_1, \ldots, c_N \in \mathbb{F}\right\}$ be the set of polynomials with coefficients from $\mathbb{F}$ and $\mathcal{P}_N^-[\mathbb{F}] := \left\{\sum_{k=1}^N c_k z^{-k} : c_1, c_2, \ldots, c_N \in \mathbb{F}\right\}$ which can be naturally identified with $\mathbb{F}^{N+1}$ and $\mathbb{F}^N$, respectively (note that $\mathcal{P}_N^+[\mathbb{F}] \cap \mathcal{P}_N^-[\mathbb{F}] = \{0\}$ according to our notation). Sometimes $[\mathbb{F}]$ is omitted because it is clear from the context.

Let $\mathcal{P}\mathcal{U}_1(m, N, \mathbb{F})$ be a set of $m \times m$ paraunitary matrix functions $U(z)$,

$$(9) \qquad\qquad \widetilde{U}(z)U(z) = I_m,$$

of the special form

$$(10) \qquad U(z) = \begin{pmatrix} u_{11}(z) & u_{12}(z) & \cdots & u_{1m}(z) \\ u_{21}(z) & u_{22}(z) & \cdots & u_{2m}(z) \\ \vdots & \vdots & \vdots & \vdots \\ u_{m-1,1}(z) & u_{m-1,2}(z) & \cdots & u_{m-1,m}(z) \\ \widetilde{u_{m1}}(z) & \widetilde{u_{m2}}(z) & \cdots & \widetilde{u_{mm}}(z) \end{pmatrix}, \quad u_{ij}(z) \in \mathcal{P}_N^+[\mathbb{F}],$$

$1 \le i, j \le m$, with determinant 1,

$$(11) \qquad\qquad \det U(z) = 1,$$

and with the linear restriction

$$(12) \qquad\qquad U(1) = I_m,$$

and such that not all polynomials u_{mj} (these are the adjoint polynomials of the entries in the last row) are zero at the origin,

$$(13) \qquad\qquad \sum_{j=1}^m |u_{mj}(0)| > 0.$$

Then for each $\mathbf{A}(z) \in \mathcal{W}\mathcal{M}_1(m, N, N, \mathbb{F})$, we have $U(z) = \text{diag}[1, \ldots, 1, z^{-N}]\mathbf{A}(z) \in \mathcal{P}\mathcal{U}_1(m, N, \mathbb{F})$ (the last row is multiplied by z^{-N}), and conversely. Thus there is a simple one-to-one correspondence

$$(14) \qquad \mathcal{W}\mathcal{M}_1(m, N, N, \mathbb{F}) \longleftrightarrow \mathcal{P}\mathcal{U}_1(m, N, \mathbb{F}),$$

and we parameterize the latter class using the following

Theorem 1. *Let $N \ge 1$. For any Laurent matrix polynomial $F(z)$ of the form*

$$(15) \qquad F(z) = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ \zeta_1(z) & \zeta_2(z) & \zeta_3(z) & \cdots & \zeta_{m-1}(z) & 1 \end{pmatrix}, \quad \zeta_j(z) \in \mathcal{P}_N^-[\mathbb{F}],$$

there exists a unique

(16) $$U(z) \in \mathcal{PU}_1(m, N, \mathbb{F})$$

such that

(17) $$F(z)U(z) \in \mathcal{P}^+(m \times m).$$

Conversely, for each $U(z)$ satisfying (16), there exists a unique matrix function $F(z)$ of the form (15) such that (17) holds.

$\mathcal{P}^+(m \times m)$ stands for the set of $m \times m$ matrix polynomials with entries from $\mathcal{P}^+$.

REMARK 2. *The relation (17) written in the equivalent form $U(z) = F^{-1}(z)M(z)$, where $M(z) \in \mathcal{P}^+(m \times m)$ and each ζ_j is replaced by $-\zeta_j$ in (15) to get $F^{-1}(z)$, means that we have the Wiener-Hopf factorization of the unitary matrix function $U(t) = U(z)|_{z=t}$ defined on $\mathbb{T}$, since $M(z)$ and $F^{-1}(z)$ are analytic regular matrix functions inside and outside (including infinity) $\mathbb{T}$, respectively. Although we heavily exploited this idea in our previous works on the factorization of matrix functions [2], [5], from which this paper has stemmed out, we tried to reduce to a minimum the application of Wiener-Hopf factorization theory in the presented proofs and discussions. This allowed us to transfer the obtained results to arbitrary subfields $\mathbb{F} \subset \mathbb{C}$ which are invariant under conjugate operation, and thus extend the area of their applications.*

The proof of Theorem 1 makes it possible to explicitly construct the corresponding $U(z)$ for a given $F(z)$, and vice versa. Namely, let the functions in (15) be

(18) $$\zeta_i(z) = \sum_{k=1}^{N} \gamma_{ik} z^{-k}, \quad i = 1, 2, \ldots, m - 1,$$

and let Θ_i be the $(N + 1) \times (N + 1)$ Hankel-like matrix

(19) $$\Theta_i = \begin{pmatrix} 0 & \gamma_{i1} & \gamma_{i2} & \cdots & \gamma_{i,N-1} & \gamma_{iN} \\ \gamma_{i1} & \gamma_{i2} & \gamma_{i3} & \cdots & \gamma_{iN} & 0 \\ \gamma_{i2} & \gamma_{i3} & \gamma_{i4} & \cdots & 0 & 0 \\ . & . & . & \cdots & . & . \\ \gamma_{iN} & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}, \quad i = 1, 2, \ldots, m - 1,$$

and

(20) $$\Delta = \sum_{i=1}^{m-1} \Theta_i \overline{\Theta}_i + I_{N+1}.$$

Assume also that B_i is the first column of Θ_i, $i = 1, 2, \ldots, m - 1$, and $B_m = (1, 0, \ldots, 0)^T$. Let $X_j = (\alpha_{j0}, \alpha_{j1}, \ldots, \alpha_{jN})^T \in \mathbb{F}^{N+1}$ be the solution of the following linear system of algebraic equations

(21) $$\Delta \cdot X = B_j, \quad j = 1, 2, \ldots, m$$

(Δ is positive definite and has a *displacement structure of rank m*, therefore $\mathrm{O}(mN^2)$ operations are required for its solution instead of traditional $\mathrm{O}(N^3)$; see [5, Appendix]),

and let

$$(22) \qquad v_{mj}(z) = \sum_{k=0}^{N} \alpha_{jk} z^{-k}, \quad j = 1, 2, \ldots, m,$$

$$(23) \qquad v_{ij}(z) = \left[\widetilde{\zeta}_i(z) v_{mj}(z) \right]^+ - \delta_{ij}, \quad i = 1, 2, \ldots, m-1,$$

where $[\, \cdot \,]^+$ stands for the projection operator, $\left[\sum_{k=-N}^{N} c_k z^k \right]^+ = \sum_{k=0}^{N} c_k z^k$. Then

$$(24) \qquad U(z) = V(z) \big(V(1) \big)^{-1},$$

where $V(z)$ is the $m \times m$ Laurent polynomial matrix $V(z) = (v_{ij}(z))_{i,j=1}^{m}$, will be the desired matrix polynomial (16) as proved in Sect. 4.

For a given $U(z)$, the corresponding $F(z)$ can be also explicitly computed as follows (see Sect. 4 for the proof): if $u_{mj}(0) \neq 0$, then

$$(25) \qquad \zeta_i(z) = \left[\frac{\widetilde{u}_{ij}(z)}{u_{mj}(z)} \right]^-, \quad i = 1, 2, \ldots, m-1,$$

where $[\, \cdot \,]^-$ stands for the projection operator: $\left[\sum_{k=-N}^{\infty} c_k z^k \right]^- = \sum_{k=-N}^{-1} c_k z^k$, and under $\frac{1}{u_{mj}(z)}$ its formal series expansion in a neighborhood of 0 is assumed. Note that we need to take only the first $N+1$ coefficients in this expansion in order to compute ζ_is.

In consequence, as the set of matrix polynomials of the form (15) can be easily identified with $\mathbb{F}^{(m-1)N}$, we have the following diagram of one-to-one and onto maps

$$(26) \qquad \mathcal{WM}_1(m, N, N, \mathbb{F}) \longleftrightarrow \mathcal{PU}_1(m, N, \mathbb{F}) \longleftrightarrow \underbrace{\mathbb{F}^N \times \mathbb{F}^N \times \ldots \times \mathbb{F}^N}_{m-1},$$

i.e. a complete parametrization of nonsingular compact wavelet matrices, which can be effectively realized.

The paper is organized as follows. In the next section we provide all notation and definitions used throughout the paper. Most of them have already been introduced in the current section but we collect them together for the convenience of reference. In Sect. 3 we reprove the factorization (7) and related facts as it seems that our approach is somewhat simpler than the traditional one. The main result of our paper, Theorem 1, is proved in Sect. 4. The essential part of this theorem, the existence of the paraunitary matrix function (16) (without showing the property (13)), has already been published (see [5, Th. 1]) for the case $\mathbb{F} = \mathbb{C}$.[1] It is sufficient to note that the proof goes through without any change if we replace $\mathbb{C}$ by $\mathbb{F}$. However, for readers' convenience, we included the simplified version of this proof in the present paper. (A minor inaccuracy of the discussion in [5] between the formulas (50) and (51) has also been corrected.)

In the remaining two sections we consider some possible applications of our method. In particular, in Sect 5, we solve the following important problem: given the first row of a wavelet matrix $\mathcal{A}$ (sometimes called the *scaling vector* or *low-pass filter*), how

---

[1]This constructive proof is a core of a new matrix spectral factorization method published in [5]. This method is currently patent pending.

to find the remaining rows of $\mathcal{A}$ (called the *wavelet vectors* or *high-pass filters*). The solution of this problem is well known and there exists an appropriate algorithm for construction of wavelet vectors (see e.g. [7, p. 64]). However this algorithm requires too many matrix multiplications which might cause the round-off problems for large m and N. We propose another algorithm for solution of this problem which uses our approach. A complete comparison of both algorithms based on numerical simulations will be provided soon.

Sect. 6 contains some discussions about other possible applications of the proposed parametrization of compact wavelet matrices.

2. Notation and Preliminaries

The fields of rational, real, and complex numbers are denoted by $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$, respectively, and $\mathbb{F}$ stands for a subfield of $\mathbb{C}$ which is invariant under the complex conjugation, $a \in \mathbb{F} \Rightarrow \overline{a} \in \mathbb{F}$.

$\mathbb{T} := \{z \in \mathbb{C} : |z| = 1\}$, $\mathbb{T}_+ := \{z \in \mathbb{C} : |z| < 1\}$, and $\mathbb{T}_- := \{z \in \mathbb{C} : |z| > 1\} \cup \{\infty\}$.

Let $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_m$ be the standard basis of $\mathbb{F}^m$, e.g., $\mathbf{e}_1 = (1, 0, \ldots, 0)$. The usual scalar product and norm in the space $\mathbb{F}^m$ are denoted by $\langle \cdot, \cdot \rangle_m$ and $\| \cdot \|_m$, respectively (they are independent of $\mathbb{F}$ as it is a subfield of $\mathbb{F}$).

Let $\mathbb{F}^{m \times n}$ be the set of $m \times n$ matrices with entries from a field $\mathbb{F}$. For $M \in \mathbb{F}^{m \times n}$, let $M^* = \overline{M}^T \in \mathbb{F}^{n \times m}$ be the Hermitian conjugate of M. $\operatorname{diag}[a_1, a_2, \ldots, a_m]$ is an $m \times m$ diagonal matrix with corresponding entries on the diagonal and $I_m = \operatorname{diag}[1, 1, \ldots, 1]$ is the $m \times m$ unit matrix. $U \in \mathbb{F}^{m \times m}$ is called unitary, $U \in \mathcal{U}_m[\mathbb{F}]$, if $UU^* = U^*U = I_m$.

If $M \in \mathbb{F}^{m \times m}$ and a is an entry of M, then $\operatorname{cof}(a) \in \mathbb{F}$ is the cofactor of a and $\operatorname{Cof}(M) \in \mathbb{F}^{m \times m}$ is the cofactor matrix, so that $M^{-1} = \frac{1}{\det M}\big(\operatorname{Cof}(M)\big)^T$ if M is nonsingular. The same notation will be used for matrix functions.

A matrix $P \in \mathbb{F}^{m \times m}$ (considered as a linear map from $\mathbb{F}^m$ to $\mathbb{F}^m$) is called the (orthogonal) projection if it is *self-adjoint*, $P = P^*$, and *idempotent*, $P^2 = P$, however we will reduce this definition to a single formula: $P = PP^*$. Note that if $P \in \mathbb{F}^{m \times m}$ is a projection of rank $r \le m$, then there exists $U \in \mathbb{C}^{m \times r}$ with orthonormal columns, $U^*U = I_r$, such that

$$(27) \qquad\qquad\qquad\qquad P = UU^*$$

(indeed, the factorization (27) with $U \in \mathbb{C}^{m \times r}$ of full rank r exists since P is nonnegative definite, and $UU^*UU^* = UU^* \Rightarrow U^*UU^*UU^*U = U^*UU^*U \Rightarrow (U^*U)^{-1} \times (U^*U)(U^*U)(U^*U)(U^*U)^{-1} = (U^*U)^{-1}(U^*U)(U^*U)(U^*U)(U^*U)^{-1} \Rightarrow U^*U = I_r$).

If P and Q from $\mathbb{F}^{m \times m}$ are projections and $P + Q = I_m$, then they are called complementary to each other. Obviously, $PQ^* = Q^*P = \mathbf{0}$ for complementary projections (as $P(I_m - P)^* = P - PP^* = \mathbf{0}$), and if P is a projection, then $I_m - P$ is also the projection complementary to P.

$\mathcal{P}[\mathbb{F}]$ denotes the set of Laurent polynomials with coefficients from a field $\mathbb{F}$, and $\mathcal{P}_N[\mathbb{F}] := \{\sum_{k=-N}^{N} c_k z^k : c_k \in \mathbb{F}, k = -N, \ldots, N\}$. If we write just $\mathcal{P}$, the field of coefficients will be clear from the context. $\mathcal{P}^+ \subset \mathcal{P}$ is the set of polynomials (with non-negative powers of z, $\sum_{k=0}^{N} c_k z^k \in \mathcal{P}^+$) and $\mathcal{P}^- \subset \mathcal{P}$ is the set of Laurent polynomials with negative powers of z, $\sum_{k=1}^{N} c_k z^{-k} \in \mathcal{P}^-$. We emphasize that, according to our

notation, constant functions belong only to $\mathcal{P}^+$ so that $\mathcal{P}^+ \cap \mathcal{P}^- = \{0\}$. Let also $\mathcal{P}_N^\pm = \mathcal{P}^\pm \cap \mathcal{P}_N$.

$\mathcal{P}(m \times n)$ denotes the set of $m \times n$ (polynomial) matrices with entries from $\mathcal{P}$, and the sets $\mathcal{P}^+(m \times n)$, $\mathcal{P}_N^-[\mathbb{F}](m \times n)$, etc. are defined similarly. The elements of these sets, $P(z) = \big(p_{ij}(z)\big)$, are called (polynomial) matrix functions. When $n = 1$ we have the vector functions and such classes are denoted by $\mathcal{P}(m)$ instead of $\mathcal{P}(m \times 1)$. When we speak about the continuous maps between these sets, we mean that they are equipped with a usual topology.

For $p(z) = \sum_{k=-N}^{N} c_k z^k \in \mathcal{P}$, let $\widetilde{p}(z) = \sum_{k=-N}^{N} \overline{c}_k z^{-k}$ and for $P(z) = [p_{ij}(z)] \in \mathcal{P}(m \times n)$ let $\widetilde{P}(z) = [\widetilde{p}_{ij}(z)]^T \in \mathcal{P}(n \times m)$. Note that $\widetilde{P}(z) = (P(z))^*$ when $z \in \mathbb{T}$. Thus usual relations for adjoint matrices like $\widetilde{P_1 + P_2}(z) = \widetilde{P}_1(z) + \widetilde{P}_2(z)$, $\widetilde{P_1 P_2}(z) = \widetilde{P}_2(z)\widetilde{P}_1(z)$, etc. hold.

We employ also the additional notation of the sets $\widetilde{\mathcal{P}_N^+}[\mathbb{F}] := \{\widetilde{p}(z) : p(z) \in \mathcal{P}_N^+[\mathbb{F}]\}$, which is an extension of $\mathcal{P}_N^-[\mathbb{F}]$, and $\mathcal{P}_N^\oplus[\mathbb{F}](m) := \underbrace{\mathcal{P}_N^+[\mathbb{F}] \times \ldots \times \mathcal{P}_N^+[\mathbb{F}] \times \widetilde{\mathcal{P}_N^+}[\mathbb{F}]}_{m}$.

A polynomial matrix (6), where $A_k \in \mathbb{F}^{m \times m}$, $k = 1, 2, \ldots, N$, is called paraunitary, we write $\mathbf{A}(z) \in \mathcal{PU}(m, N, \mathbb{F})$, if (4) holds, which is equivalent to $\sum_{k=0}^{N-l} A_k A_{k+l}^* = \delta_{l0} I_m$, $l = 0, 1, \ldots, N$. This means that $\mathcal{A} = (A_0, A_1, A_2, \cdots, A_N) \in \mathbb{F}^{m \times m(N+1)}$ is a wavelet matrix and we do not make distinction between $\mathcal{A}$ and its its polyphase representation (6). If $A_N \neq \mathbf{0}$ in the representation (6), then we say that the wavelet matrix $\mathcal{A} \equiv \mathbf{A}(z)$ has rank m and order N, we write $\mathbf{A}(z) \in \mathcal{WM}(m, N, \mathbb{F})$. The degree of a wavelet matrix $\mathbf{A}(z)$ is the order of a monomial $\det \mathbf{A}(z)$, i.e. $\det \mathbf{A}(z) = c \cdot z^{\deg(\mathcal{A})}$. The set of wavelet matrices of rank m, order N, and degree d will be denoted by $\mathcal{WM}(m, N, d, \mathbb{F})$. In addition, $\mathcal{WM}_0(m, N, d, \mathbb{F})$ is the subset of wavelet matrices which satisfy (5), and $\mathbf{A}(z) \in \mathcal{WM}_1(m, N, d, \mathbb{F}) \subset \mathcal{WM}_0(m, N, d, \mathbb{F})$ if the last row of A_N differs from the zero row vector.

Recall also that $\mathcal{PU}_1(m, N, \mathbb{F})$ denotes the set of specific paraunitary matrix functions which satisfy (9)–(13).

For power series $f(z) = \sum_{k=-\infty}^{\infty} c_k z^k$ and $N \geq 1$, let $[f(z)]^-$, $[f(z)]^+$, $[f(z)]_N^-$, and $[f(z)]_N^+$, denote respectively $\sum_{k=-\infty}^{-1} c_k z^k$, $\sum_{k=0}^{\infty} c_k z^k$, $\sum_{k=-N}^{-1} c_k z^k$, and $\sum_{k=0}^{N} c_k z^k$ and the corresponding functions are assumed under these expressions if the convergence domains of these power series are clear from the context (the dependence of coefficients c_k on the function f is sometimes expressed by $c_k\{f\} = c_k$). Obviously $[f]^- = f - [f]^+$ under these notation.

A matrix function $S(z) \in \mathcal{P}[\mathbb{C}](m \times m)$ is called positive definite if $S(z)$ is such $(XS(z)X^* > 0$ for each $0 \neq X \in \mathbb{C}^{1 \times m})$ for almost every $z \in \mathbb{T}$. The polynomial matrix spectral factorization theorem (see e.g. [3]) asserts that every positive definite $S(z) \in \mathcal{P}_N(m \times m)$ can be factorized as

$$(28) \qquad S(z) = S^+(z)\widetilde{S^+}(z), \quad z \in \mathbb{C}\backslash\{0\},$$

where $S^+ \in \mathcal{P}_N^+(m \times m)$ and $\det S^+(z) \neq 0$ for each $z \in \mathbb{T}_+$ (consequently, $\widetilde{S^+}(z)$ is analytic and invertible in $\mathbb{T}_-$), and the representation (28) is unique in a sense that

if $S(z) = S_1^+(z)\widetilde{S_1^+}(z)$ is another spectral factorization of $S(z)$, then $S_1^+(z) = S^+(z)U$ for some unitary $U \in \mathcal{U}_m$.

3. Wavelet Matrix Factorization Theorem

The material of this section is mostly well known, however we provide compact proofs of the given statements making emphasis on arbitrariness of a field $\mathbb{F}$.

Lemma 1. *Let*

$$(29) \qquad \mathbf{A}(z) = \sum_{k=0}^{N} A_k z^k, \quad A_k \in \mathbb{F}^{m \times m}, \ \ A_N \neq 0,$$

be a wavelet matrix of rank m, order N and degree d, $\mathbf{A}(z) \in \mathcal{WM}(m, N, d, \mathbb{F})$. Then
  a) $d \geq N$;
  b) $d = N$ *if and only if* $\mathrm{rank}(A_0) = m - 1$.

Proof. We have

$$\sum_{k=0}^{N} A_k^* z^{-k} = \widetilde{\mathbf{A}}(z) = \mathbf{A}^{-1}(z) = \frac{1}{\det \mathbf{A}(z)} \big(\mathrm{Cof}\, \mathbf{A}(z) \big)^T = c z^{-d} \big(\mathrm{Cof}\, \mathbf{A}(z) \big)^T,$$

and since $\mathrm{Cof}\,\mathbf{A}(z) \in \mathcal{P}^+(m \times m)$ and $A_N \neq 0$, the equation $\sum_{k=0}^{N} A_k^* z^{-k} = \frac{c}{z^d}\big(\mathrm{Cof}\, \mathbf{A}(z) \big)^T$ implies a). Using the same reasoning, we conclude that $\mathrm{rank}(A_0) < m - 1 \iff \mathrm{Cof}(A_0) = \mathbf{0} \iff d > N$ (note that if $\mathrm{Cof}\,\mathbf{A}(z) = \sum_{k=0}^{N} C_k z^k$, then $C_0 = \mathrm{Cof}(A_0)$). Hence b) follows as well (recall that $\mathrm{rank}(A_0) \neq m$ since $A_0 A_N^* = 0$). $\qquad \square$

The following lemma will be used in the sequel only for $d = 1$.

Lemma 2. (cf. [6, Th. 3.1]). *Let* $\mathbf{V}(z) = Q + Pz$, $P, Q \in \mathbb{F}^{m \times m}$, *be a matrix polynomial. Then it is a wavelet matrix of rank m, order 1 and degree d satisfying $V(1) = I_m$, $\mathbf{V}(z) \in \mathcal{WM}_0(m, 1, d, \mathbb{F})$, if and only if P and Q are complementary projections on $\mathbb{F}^m$ and $\mathrm{rank}(P) = d$.*

Proof. The first part of the lemma can be proved by observation that $(Q + Pz)(Q^* + P^*z) = I_m$ and $\mathbf{V}(1) = I_m \iff PQ^* = 0$, $PP^* + QQ^* = I_m$, and $P + Q = I_m \iff P$ and Q are complementary projections.

Now the property of P to be a projection is equivalent to the existence of $U \in \mathbb{C}^{m \times d}$, $\mathrm{rank}(U) = \mathrm{rank}(P) = d$, with orthonormal columns, $U^*U = I_d$, such that (27) holds. Let $U_0 \in \mathbb{C}^{m \times m}$ be any unitary matrix which completes the columns of U. Then

$$U_0^* V(z) U_0 = U_0^*(I - UU^* + UU^*z)U_0 = \mathrm{diag}[\underbrace{z, z, \ldots, z}_{d}, \underbrace{1, 1, \ldots, 1}_{m-d}]$$

whose determinant is z^d. Hence the lemma is proved. $\qquad \square$

Theorem 2. (see [7, Th. 4.4.15]). *Let $\mathbf{A}(z)$ be a wavelet matrix of rank m and of order and degree N satisfying the linear condition (5), $\mathbf{A}(z) \in \mathcal{WM}_0(m, N, N, \mathbb{F})$. Then there exists a unique factorization (7).*

Proof. By virtue of Lemma 1, $\text{rank}(A_0) = m-1$. Let a nonzero column vector $v \in \mathbb{F}^m$ be orthogonal to the columns of A_0, $v^*A_0 = 0$, and $\mathbf{V}_1(z) = I_m - P + Pz$, where $P = v(v^*v)^{-1}v^*$ is the projection. Then $\mathbf{V}_1(z) \in \mathcal{WM}_0(m,1,1,\mathbb{F})$ and $\mathbf{V}_1(z)$ divides $\mathbf{A}(z)$ on the left (the quotient $\mathbf{B}(z) := \mathbf{V}_1^{-1}(z)\mathbf{A}(z) = \widetilde{\mathbf{V}_1}(z)\mathbf{A}(z) \in \mathcal{P}^+(m \times m)$ as $P^*A_0 = 0$).

As $\deg(\mathbf{B}) = \deg(\mathbf{A}) - \deg(\mathbf{V}_1) = N-1$ and $\deg(\mathbf{B}) \geq \text{ord}(\mathbf{B})$ by virtue of Lemma 1, we have $\text{ord}(\mathbf{B}) = N-1$ (obviously, it cannot be less than $N-1$ as $\mathbf{V}_1(z)\mathbf{B}(z) = \mathbf{A}(z)$). Hence $\mathbf{B}(z) \in \mathcal{WM}_0(m, N-1, N-1, \mathbb{F})$ and if we continue these divisions, we get the factorization (7).

The uniqueness of a divisor $\mathbf{V}_1(z)$ (and hence of other factors) follows from the fact that if $\mathbf{V}_1(z) = Q + Pz \in \mathcal{WM}_0(m,1,1,\mathbb{F})$, where P and Q are complementary projections and $\text{rank}(P) = 1$ (see Lemma 2), then $PA_0 = 0$ as $\mathbf{V}_1^{-1}(z)\mathbf{A}(z) = (Pz^{-1} + Q)\mathbf{A}(z)$ does not have the coefficient at z^{-1}, and since $\text{rank}(A_0) = m-1$, such a projection P is unique. $\qquad\square$

4. PROOF OF THE MAIN RESULT

We introduce the following system of m conditions which plays a key role in the proof of Theorem 1 (where this system comes from is explained in [4, Lemma 5]) . Namely, for given Laurent polynomials

$$(30) \qquad\qquad \zeta_j(z) \in \mathcal{P}_N^-[\mathbb{F}], \quad j = 1, 2, \ldots, m-1,$$

let

$$(31) \qquad \begin{cases} \zeta_1(z)x_m(z) - \widetilde{x_1}(z) \in \mathcal{P}^+, \\ \zeta_2(z)x_m(z) - \widetilde{x_2}(z) \in \mathcal{P}^+, \\ \vdots \\ \zeta_{m-1}(z)x_m(z) - \widetilde{x_{m-1}}(z) \in \mathcal{P}^+, \\ \zeta_1(z)x_1(z) + \zeta_2(z)x_2(z) + \ldots + \zeta_{m-1}(z)x_{m-1}(z) + \widetilde{x_m}(z) \in \mathcal{P}^+. \end{cases}$$

We say that a vector function

$$(32) \quad \mathbf{u}(z) = \big(u_1(z), u_2(z), \ldots, u_{m-1}(z), \widetilde{u_m}(z)\big)^T, \quad u_i(z) \in \mathcal{P}_N^+[\mathbb{F}], \; i = 1, 2, \ldots, m,$$

(we emphasize that the first $m-1$ entries of (32) belong to $\mathcal{P}_N^+[\mathbb{F}]$ and the last entry belongs to $\widetilde{\mathcal{P}_N^+}[\mathbb{F}]$) is a solution of (31) if and only if all the conditions in (31) are satisfied whenever $x_i(z) = u_i(z)$, $i = 1, 2, \ldots, m$ (it is assumed that $\widetilde{x_m}(z) = \widetilde{u_m}(z)$). Observe that the set of solutions of (31) is a linear subspace of $\mathcal{P}_N^\oplus[\mathbb{F}](m) := \underbrace{\mathcal{P}_N^+[\mathbb{F}] \times \ldots \times \mathcal{P}_N^+[\mathbb{F}] \times \widetilde{\mathcal{P}_N^+}[\mathbb{F}]}_{m}$. We will see that actually this subspace is always m dimensional.

We make essential use of the following

Lemma 3. *Let (30) hold, and let*

$$(33) \qquad\qquad \mathbf{u}(z) = \big(u_1(z), u_2(z), \ldots, u_{m-1}(z), \widetilde{u_m}(z)\big)^T \in \mathcal{P}_N^\oplus[\mathbb{F}](m),$$

and

$$(34) \qquad \mathbf{v}(z) = \big(v_1(z), v_2(z), \ldots, v_{m-1}(z), \widetilde{v_m}(z)\big)^T \in \mathcal{P}_N^{\oplus}[\mathbb{F}](m),$$

be two (*possibly the same*) *solutions of the system* (*31*). *Then* $\langle \mathbf{u}(z), \mathbf{v}(z) \rangle_m$ *is the same for every* $z \in \mathbb{C} \backslash \{0\}$, *i.e.*

$$(35) \qquad \sum_{i=1}^{m-1} u_i(z)\widetilde{v}_i(z) + \widetilde{u_m}(z)v_m(z) = \text{Const}.$$

Proof. Substituting $x_i = v_i$ in the first $m - 1$ conditions and $x_i = u_i$ in the last condition of (31), and then multiplying the functions in the first $m - 1$ conditions by u_i and the function in the last condition by v_m, we get

$$\begin{cases} \zeta_1 v_m u_1 - \widetilde{v}_1 u_1 \in \mathcal{P}^+, \\ \zeta_2 v_m u_2 - \widetilde{v}_2 u_2 \in \mathcal{P}^+, \\ \vdots \\ \zeta_{m-1} v_m u_{m-1} - \widetilde{v_{m-1}} u_{m-1} \in \mathcal{P}^+, \\ \zeta_1 u_1 v_m + \zeta_2 u_2 v_m + \ldots + \zeta_{m-1} u_{m-1} v_m + \widetilde{u_m} v_m \in \mathcal{P}^+. \end{cases}$$

Subtracting the first $m - 1$ functions from the last function in the latter system, we get

$$(36) \qquad \sum_{i=1}^{m-1} u_i(z)\widetilde{v}_i(z) + \widetilde{u_m}(z)v_m(z) \in \mathcal{P}^+.$$

We can interchange the roles of u and v in the above discussion to get in a similar manner that

$$(37) \qquad \sum_{i=1}^{m-1} v_i(z)\widetilde{u}_i(z) + \widetilde{v_m}(z)u_m(z) \in \mathcal{P}^+.$$

It follows from the relations (36) and (37) that the function in (35) and its adjoint belong to $\mathcal{P}^+$, which implies (35). $\qquad \square$

COROLLARY 1. *If* (*33*) *and* (*34*) *are two solutions of the system* (*31*), *and*

$$(38) \qquad \mathbf{u}(1) = \mathbf{v}(1),$$

then

$$(39) \qquad \mathbf{u}(z) = \mathbf{v}(z) \quad \text{for each } z \in \mathbb{C} \backslash \{0\}.$$

In particular, if $\mathbf{u}(1) = \mathbf{0} \in \mathbb{F}^m$, *then* $\mathbf{u}(z) = \mathbf{0}$ *for each* $z \in \mathbb{C} \backslash \{0\}$ *since the trivial vector function* $\mathbf{v}(z) = \mathbf{0}$ *is always a solution of the system* (*31*).

Proof. Since $\mathbf{u}(z) - \mathbf{v}(z)$ is also a solution of (31), it follows from the lemma that $\|\mathbf{u}(z) - \mathbf{v}(z)\|_m = \|\mathbf{u}(1) - \mathbf{v}(1)\|_m = 0$ for each $z \in \mathbb{C} \backslash \{0\}$. Hence (39) holds. $\qquad \square$

REMARK 3. *One can see that Corollary 1 remains valid if we take any fixed point* $z_0 \neq 0$ *in the role of 1 in the equation* (*38*).

Lemma 4. *Let* (*30*) *hold, and let vector functions*

$$(40) \qquad \mathbf{v}_j(z) = \big(v_{1j}(z), v_{2j}(z), \ldots, \widetilde{v_{mj}}(z)\big)^T \in \mathcal{P}_N^{\oplus}[\mathbb{F}](m), \quad j = 1, 2, \ldots, m,$$

be any m solutions of the system (*31*). *Then the determinant of the $m \times m$ Laurent polynomial matrix*

$$(41) \qquad\qquad\qquad V(z) = (\mathbf{v}_1(z), \mathbf{v}_2(z), \ldots \mathbf{v}_m(z))$$

is constant

$$(42) \qquad\qquad\qquad \det V(z) = \mathrm{Const.}, \quad z \in \mathbb{C} \backslash \{0\}.$$

Proof. Since the vector polynomials (40) satisfy the last condition of the system (31), we have

$$(43) \qquad\qquad\qquad F(z)V(z) \in \mathcal{P}^+(m \times m),$$

where $F(z)$ is defined by (15). Consequently, as $\det F(z) = 1$,

$$(44) \qquad\qquad\qquad \det V(t) \in \mathcal{P}^+.$$

Since the vector polynomials (40) satisfy the first $m-1$ conditions of the system (31), we have

$$\phi_{ij}(z) := \zeta_i(z)v_{mj}(z) - \widetilde{v_{ij}}(z) \in \mathcal{P}^+,$$

$1 \le j \le m$, $1 \le i < m$. Direct computations show that

$$\widetilde{V}(z)F^{-1}(z) = \Phi(z) \in \mathcal{P}^+(m \times m),$$

where $F^{-1}(z)$ is obtained from $F(z)$ by replacing each ζ_i by $-\zeta_i$ and

$$\Phi(z) = \begin{pmatrix} -\phi_{11}(z) & -\phi_{21}(z) & \cdots & -\phi_{m-1,1}(z) & v_{m1}(z) \\ -\phi_{12}(z) & -\phi_{22}(z) & \cdots & -\phi_{m-1,2}(z) & v_{m2}(z) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -\phi_{m1}(z) & -\phi_{m1}(z) & \cdots & -\phi_{m-1,m}(z) & v_{m,m}(z) \end{pmatrix}.$$

Consequently $\det \widetilde{V}(z) = \det \Phi(z) \in \mathcal{P}^+$ and together with (44) this gives (42). $\qquad \square$

REMARK 4. *Observe that the relation* (*43*) *holds under the hypothesis of the lemma.*

Now we construct explicitly m independent solutions (40) of the system (31). We seek for a nontrivial solution

$$(45) \qquad\qquad \mathbf{x}(z) = \big(x_1(z), x_2(z), \ldots, \widetilde{x_m}(z)\big)^T \in \mathcal{P}_N^{\oplus}[\mathbb{F}](m)$$

of (31), where

$$(46) \qquad\qquad x_i(z) = \sum_{k=0}^{N} \alpha_{ik} z^k, \quad i = 1, 2, \ldots, m,$$

and the coefficients a_{ik} are to be determined.

Equating the coefficients of z^{-k}, $k = 0, 1, 2, \ldots, N$ of the Laurent polynomials in the system (31) to 0, except the 0th coefficient of the jth function which we equate to

1, we get the following system of algebraic equations in the block matrix form which we denote by $\mathbb{S}_j$:

(47)
$$\mathbb{S}_j := \begin{cases} \Theta_1 X_m - \overline{X_1} = \mathbf{0}, \\ \Theta_2 X_m - \overline{X_2} = \mathbf{0}, \\ \vdots \\ \Theta_j X_m - \overline{X_j} = \mathbf{1}, \\ \vdots \\ \Theta_{m-1} X_m - \overline{X_{m-1}} = \mathbf{0}, \\ \Theta_1 X_1 + \Theta_2 X_2 + \ldots + \Theta_{m-1} X_{m-1} + \overline{X_m} = \mathbf{0}, \end{cases}$$

where Θ_i is defined from the equations (19) and (18), $\mathbf{0} = (0, 0, \ldots, 0)^T \in \mathbb{F}^{N+1}$, $\mathbf{1} = (1, 0, 0, \ldots, 0)^T \in \mathbb{F}^{N+1}$, and the column vectors

(48)
$$X_i = (\alpha_{i0}, \alpha_{i1}, \ldots, \alpha_{iN})^T, \quad i = 1, 2, \ldots, m,$$

(see (46)) are unknown.

REMARK 5. *We emphasize that if $(X_1, X_2, \ldots, X_m)$ defined by (48) is the solution of the system (47), then the vector function (45) defined by (46) will be the solution of the system (31).*

It is easy to show that the system (47) $\mathbb{S}_j$ has a solution for each $j = 1, 2, \ldots, m$. Indeed, determining X_i, $i = 1, 2, \ldots, m - 1$, from the first $m - 1$ equations in (47),

(49)
$$X_i = \overline{\Theta_i} \cdot \overline{X_m} - \delta_{ij} \mathbf{1}, \quad i = 1, 2, \ldots, m - 1,$$

and then substituting into the last equation of (47), we get

$$\Theta_1 \cdot \overline{\Theta_1} \cdot \overline{X_m} + \Theta_2 \cdot \overline{\Theta_2} \cdot \overline{X_m} + \ldots + \Theta_{m-1} \cdot \overline{\Theta_{m-1}} \cdot \overline{X_m} + \overline{X_m} = \Theta_j \cdot \mathbf{1}$$

(we assume that $\Theta_m = I_{N+1}$, i.e. the right-hand side is equal to $\mathbf{1}$ when $j = m$) or, equivalently,

(50)
$$(\Theta_1 \cdot \overline{\Theta_1} + \Theta_2 \cdot \overline{\Theta_2} + \ldots + \Theta_{m-1} \cdot \overline{\Theta_{m-1}} + I_{N+1}) \cdot \overline{X_m} = \Theta_j \cdot \mathbf{1}.$$

This is the same system as (21) (see 20). Since each Θ_i is symmetric, $\Theta_i = \Theta_i^T$, we have that $\Theta_i \overline{\Theta_i} = \Theta_i \Theta_i^*$, $i = 1, 2, \ldots, m - 1$, are non-negative definite and the coefficient matrix (20) of the system (50) (which is the same for each $j = 1, 2, \ldots, m$) is positive definite (with all eigenvalues larger than or equal to 1). Consequently, Δ is nonsingular, $\det \Delta \geq 1$, and the system (50) has a unique solution for each j.

Finding the vector $\overline{X_m} \in \mathbb{F}^{N+1}$ from (50) and then determining $X_1, X_2, \ldots, X_{m-1}$ from (49), we get the unique solution of $\mathbb{S}_j$. To indicate its dependence on j, we denote the solution of $\mathbb{S}_j$ by $(X_1^j, X_2^j, \ldots, X_{m-1}^j, X_m^j)$,

(51)
$$X_i^j := (\alpha_{i0}^j, \alpha_{i1}^j, \ldots, \alpha_{iN}^j)^T, \quad i = 1, 2, \ldots, m,$$

so that the vector functions (40), where

$$v_{ij}(z) = \sum_{k=0}^{N} \alpha_{ik}^j z^k, \quad 1 \leq i, j \leq m,$$

are m solutions of the system (31) (see Remark 5). These vector functions $\mathbf{v}_1(z)$, $\mathbf{v}_2(z)$, ..., $\mathbf{v}_m(z)$ are linearly independent since the linear transformation $\mathbf{L} : \mathcal{P}_N^{\oplus}[\mathbb{F}](m) \to \mathbb{F}^m$ which maps $(x_1(z), x_2(z), \ldots, \widetilde{x_m}(z))$ into the 0th coefficients of the functions (or their adjoints) standing on the left-hand side of the system (31), viz. into $\big(c_0\{\widetilde{\zeta_1}(z)\widetilde{x_m}(z) - x_1(z)\}, c_0\{\widetilde{\zeta_2}(z)\widetilde{x_m}(z) - x_2(z)\}, \ldots, c_0\{\zeta_1(z)x_1(z) + \zeta_2(z)x_2(z) + \ldots + \widetilde{x_m}(z)\}\big)$, transforms m vector functions $\mathbf{v}_1(z)$, $\mathbf{v}_2(z)$, ..., $\mathbf{v}_m(z)$ into linearly independent standard bases of $\mathbb{F}^m$. Namely, $\mathbf{L}\big(\mathbf{v}_i(z)\big) = (\delta_{i1}, \delta_{i2}, \ldots, \delta_{im})$, $i = 1, 2, \ldots, m$, because of (47). Consequently $V(1)$ is nonsingular (see (41)) since if $\mathbf{w} \cdot V(1) = \mathbf{0} \in \mathbb{F}^m$ for some $\mathbf{0} \neq \mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{F}^m$, then $\mathbf{w} \cdot V(z) = \sum_{k=1}^{m} w_k \mathbf{v}_k(z) = \mathbf{0}$ by virtue of Corollary 1 of Lemma 3, which contradicts the independence of $\mathbf{v}_1(z)$, $\mathbf{v}_2(z), \ldots, \mathbf{v}_m(z)$.

Let $U(z)$ be defined by (24). Then it has the form (10) and its column vectors $\mathbf{u}_1(z)$, $\mathbf{u}_2(z), \ldots, \mathbf{u}_m(z)$,

$$(52) \qquad\qquad U(z) = (\mathbf{u}_1(z), \mathbf{u}_2(z), \ldots, \mathbf{u}_m(z)),$$

are m solutions of (31) satisfying

$$(53) \qquad\qquad \mathbf{u}_i(1) = \mathbf{e}_i, \quad i = 1, 2, \ldots, m,$$

(since (12) holds because of (24)). Therefore, the matrix function $U(z)$ is paraunitary since $\widetilde{U}(z)U(z)$ is a constant matrix, by virtue of Lemma 3, and this constant is I_m since (12) holds. By virtue of Lemma 4, the determinant of $U(z)$ is also a constant which is equal to 1 since $\det u(1) = 1$. Hence the relations (9)–(12) are valid for (52). Observe also that (17) holds because of (43) (see Remark 4) and (24). Hence it remains to show only the relation (13) in order to complete the proof of the first part of Theorem 1. Meanwhile we are ready to formulate and prove a corollary of the above discussion which will be used in the next section.

COROLLARY 2. *Let (30) hold, let $F(z)$ be the matrix function defined by (15), and let (52) be the corresponding (according to Theorem 1) $U(z) \in \mathcal{PU}_1(m, N, \mathbb{F})$.*

If $\mathbf{b} = (b_1, b_2, \ldots, b_m) \in \mathbb{F}^m$, then $\mathbf{u_b}(z)$ is a solution of the system (31) satisfying

$$\mathbf{u_b}(1) = \mathbf{b},$$

if and only if

$$\mathbf{u_b}(z) = \sum_{i=1}^{m} b_i \, \mathbf{u}_i(z), \quad z \in \mathbb{C}\backslash\{0\}.$$

Proof. Since $\mathbf{u}_1(z), \mathbf{u}_2(z), \ldots, \mathbf{u}_m(z)$ (see (52)) are solutions of the system (31) (recall that the set of its solutions is a linear subspace) and (53) holds, the first part of the corollary is clear. The second part follows from the first part and from Corollary 1. $\square$

In order to prove (13), let

$$(54) \qquad\qquad \Psi(z) = \big(\psi_{ij}(z)\big)_{i,j=1}^{m} := F(z)U(z),$$

which, as has already been mentioned, belongs to $\mathcal{P}^+(m \times m)$ (see (17)). Since the determinants of $F(z)$ and $U(z)$ are 1 for each $z \in \mathbb{C}\backslash\{0\}$, we can conclude that

$$(55) \qquad\qquad \det \Psi(z) = 1 \quad \text{for each } z \in \mathbb{C}.$$

Because of the structure of the matrix (15), we have

$$\psi_{ij}(z) = u_{ij}(z), \quad 1 \le i < m, \ 1 \le j \le m.$$

Since $\widetilde{U}(z) = U^{-1}(z)$ and (11) holds, we have

$$u_{mj}(z) = \operatorname{cof} u_{mj}(z) = \operatorname{cof} \psi_{mj}(z), \quad 1 \le j \le m.$$

Thus, by virtue of (55),

$$1 = \det \Psi(z) = \sum_{j=1}^{m} \psi_{mj}(z) \operatorname{cof} \psi_{mj}(z) = \sum_{j=1}^{m} \psi_{mj}(z) u_{mj}(z)$$

for each $z \in \mathbb{C}$ including 0. Consequently (13) holds.

Thus, the constructed matrix function $U(z)$ has all the desired properties, i.e. (16) and (17) hold. Note that a brief way of construction of the entries of $U(z)$ is described by the formulas (18)–(24).

The uniqueness of (16) follows from the uniqueness of spectral factorization (see Section 2) since $F(z)U(z)$ is the spectral factor of $F(z)\widetilde{F}(z)$.

Let us now show the converse part of Theorem 1. If we have a matrix function (16), then $u_{mj}(0) \ne 0$ for some j since (13) holds. Let us determine functions ζ_i by the formula (25), construct the matrix function (15), and show that (17) is valid. For this we need only to check that the entries of the last row of $\Psi(z)$ (see (54)) belong to $\mathcal{P}^+[\mathbb{F}]$. For $1 \le n \le m$, we have

$$\mathcal{P} \ni \sum_{i=1}^{m-1} \zeta_i(z) u_{in}(z) + \widetilde{u_{mn}}(z) = \sum_{i=1}^{m-1} \left(\frac{\widetilde{u}_{ij}(z)}{u_{mj}(z)} - \left[\frac{\widetilde{u}_{ij}(z)}{u_{mj}(z)} \right]^+ \right) u_{in}(z) + \widetilde{u_{mn}}(z) =$$

(56) $$\frac{1}{u_{mj}(z)} \left(\sum_{i=1}^{m-1} \widetilde{u}_{ij}(z) u_{in}(z) + u_{mj}(z) \widetilde{u_{mn}}(z) \right) - \sum_{i=1}^{m-1} \left[\frac{\widetilde{u}_{ij}(z)}{u_{mj}(z)} \right]^+ u_{in}(z) =$$

$$\frac{\delta_{nj}}{u_{mj}(z)} - \sum_{i=1}^{m-1} \left[\frac{\widetilde{u}_{ij}(z)}{u_{mj}(z)} \right]^+ u_{in}(z),$$

which is analytic in a neighborhood of 0 and yields that this function belongs to $\mathcal{P}^+$. Thus (17) holds.

Let us now show the uniqueness of the desired $F(z)$.

Recall that $F^{-1}(z)$ can be obtained by replacing each ζ_i by $-\zeta_i$ in (15). Hence $F^{-1}(z) \in \widetilde{\mathcal{P}_N^+}[\mathbb{F}](m \times m)$. Since $\Psi(z) \in \mathcal{P}^+(m \times m)$ (see (54) and (17)) and (55) holds, we have $\Psi^{-1}(z) \in \mathcal{P}^+(m \times m)$.

If $F_1(z)$ has the same form (15) with the last row $[\zeta_1'(z), \zeta_2'(z), \ldots, \zeta_{m-1}'(z), 1]$ and $\Psi_1(z) := F_1(z)U(z) \in \mathcal{P}^+(m \times m)$, then $U(z) = F^{-1}(z)\Psi(z) = F_1^{-1}(z)\Psi_1(z)$, which yields

$$\widetilde{\mathcal{P}^+}(m \times m) \ni F_1(z) F^{-1}(z) = \Psi_1(z) \Psi^{-1}(z) \in \mathcal{P}^+(m \times m).$$

Thus $F_1(z) F^{-1}(z)$ is a constant matrix while, on the other hand, this product has the form (15) with the last row $[\zeta_1' - \zeta_1, \zeta_2' - \zeta_2, \ldots, \zeta_{m-1}' - \zeta_{m-1}, 1]$, which implies that $\zeta_i' = \zeta_i$, $i = 1, 2, \ldots, m-1$.

5. Wavelet Matrices with Given First Rows

If we know the first row of the wavelet matrix (7), then one can uniquely determine each P_i and Q_i in (7) and then recover $\mathbf{A}(z)$ by the formula (7), i.e. find the remaining $m-1$ rows of $\mathbf{A}(z)$. The algorithm for this procedure is well known (see e.g. [7, Th. 4.4.17]). We describe a new method of reconstruction of $\mathbf{A}(z)$ based on the proposed parametrization of compact wavelet matrices. This description is included in a constructive proof of the following

Theorem 3. *Let* $\mathrm{v} = (v_1, v_2, \ldots, v_m) \in \mathbb{F}^m$ *be a vector of the unit norm and* $V \in \mathbb{F}^{m \times m}$ *be a unitary matrix with the first row* v. *If* $\mathbf{A}_1(z) = \big(a_{11}(z), a_{12}(z), \ldots, a_{1m}(z)\big) \in \mathcal{P}_N^+(1 \times m)$ *is a row function of order* N $\big(\sum_{j=1}^m |\alpha_{Nj}| > 0$, *where* $a_{1j}(z) = \sum_{k=0}^N \alpha_{kj} z^k$, $j = 1, 2, \ldots, m\big)$ *such that* $\mathbf{A}_1(z)\widetilde{\mathbf{A}_1}(z) = I_m$, $z \in \mathbb{C}\backslash\{0\}$ *and*

(57) $$\mathbf{A}_1(1) = \mathrm{v},$$

then there exists a unique wavelet matrix of rank m *and of order and degree* N, $\mathbf{A}(z) \in \mathcal{WM}(m, N, N, \mathbb{F})$, *with* $\mathbf{A}(1) = V$ *which has the first row* $\mathbf{A}_1(z)$.

REMARK 6. *For a given* $\mathrm{v} \in \mathbb{F}^m$ *with* $\|\mathrm{v}\|_m = 1$, *it is in general hard to decide whether there exists a unitary matrix* $V \in \mathbb{F}^{m \times m}$ *with the first row* v *(because of the arbitrariness of the field* $\mathbb{F}$ *which not always contains* $\sqrt{a}$ *for a positive* $a \in \mathbb{F}$*). However the theorem can be always used for* $\mathrm{v} = \mathbf{e}_1$ *and* $V = I_m$.

Proof. For notational convenience, we will find $\mathbf{A}^T(z)$ instead of $\mathbf{A}(z)$. Thus we assume that the $\mathrm{v} = (v_1, v_2, \ldots, v_m)^T$ is a column vector and $\mathbf{A}_1(z) = \big(a_{11}(z), \ldots, a_{1m}(z)\big)^T \in \mathcal{P}_N^+(m \times 1)$, which satisfies $\widetilde{\mathbf{A}_1}(z)\mathbf{A}_1(z) = I_m$ and (57). Furthermore, without loss of generality (we interchange the rows if necessary), we assume that $\alpha_{Nm} \neq 0$ where we recall $a_{1m}(z) = \sum_{k=0}^N \alpha_{km} z^k$.

Consider now $\mathbf{U}_1(z) = \big(u_{11}(z), u_{21}(z), \ldots, \widetilde{u_{m1}}(z)\big)^T \in \mathcal{P}_N^\oplus(m)$, where $u_{j1}(z) = a_{1j}(z)$, $j = 1, 2, \ldots, m-1$, and $\widetilde{u_{m1}}(z) = z^{-N}a_{1m}(z)$. Then $u_{m1}(0) \neq 0$, and we can define ζ_i, $i = 1, 2, \ldots, m-1$, by a formula like (25)

$$\zeta_i(z) = \left[\frac{\widetilde{u}_{i1}(z)}{u_{m1}(z)}\right]^- = \left[\frac{\widetilde{u}_{i1}(z)}{u_{m1}(z)}\right]_N^-, \quad i = 1, 2, \ldots, m-1,$$

and construct the matrix function $F(z)$ defined by (15). Consider now the corresponding (according to Theorem 1) $U(z) \in \mathcal{PU}_1(m, N, \mathbb{F})$ whose columns $\mathbf{u}_1(z)$, $\mathbf{u}_2(z)$, $\ldots, \mathbf{u}_m(z)$, as we remember, are solutions of the system (31) and also satisfy (53). We can make sure by direct computations like (56) that $U_1(z)$ satisfies the last condition of (31), and taking into account the relations

$$\zeta_i(z)u_{m1}(z) - \widetilde{u_{i1}}(z) = \left(\frac{\widetilde{u}_{i1}(z)}{u_{m1}(z)} - \left[\frac{\widetilde{u}_{i1}(z)}{u_{m1}(z)}\right]^+\right)u_{m1}(z) - \widetilde{u_{i1}}(z) = -\left[\frac{\widetilde{u}_{i1}}{u_{m1}}\right]^+ u_{m1} \in \mathcal{P}^+,$$

$i = 1, 2, \ldots, m - 1$, we see that $U_1(z)$ is a solution of the system (31). Consequently, according to Corollary 2,

$$U_1(z) = U(z) \cdot \mathrm{v} = \sum_{i=1}^{m} v_i \, \mathbf{u}_i(z),$$

(as this equation holds for $z = 1$) and it is the first column of $U(z) \cdot V$. This matrix function is paraunitary as well (since V is unitary) and satisfies the condition $U(1)V = V$. Hence

$$\mathbf{A}(z) = \mathrm{diag}[1, 1, \ldots, 1, z^N] U(z) V$$

will be the desired matrix.

The uniqueness of $\mathbf{A}(z)$ is also valid since $F(z)$ described in the above proof is the same as the matrix function corresponding to $\mathbf{A}(z) \cdot V^{-1} \in \mathcal{WM}_1(m, N, N, \mathbb{F})$ by the to one-to-one map (14) and Theorem 1, and such $F(z)$ is unique. $\qquad \square$

6. Other Possible Applications

In the end, we would like to discuss briefly some possible applications of the proposed method of compact wavelet matrices construction. It should be emphasized that the intent of this section is largely motivational and we consider three separate topics.

A. Rational approximations to compact wavelet matrices. Most of compact wavelet matrices used in practice, for example Daubechies wavelet matrices, obey certain additional restrictions. The proofs of the existence of such matrices and the ways of their construction are highly non-linear and thus the obtained coefficients are in general irrational. In actual calculations on a digital computer, these coefficients should be quantized and hence approximated by rational numbers. It may happen during this approximation that the basic property of the wavelet matrices (2) will not be preserved exactly. Using the proposed parametrization and taking $\mathbb{Q}$ in the role of $\mathbb{F}$, we can provide an approximation of any compact wavelet matrix $\mathcal{A}$ by $\mathcal{A}'$ with rational coefficients preserving exactly the shifted orthogonality condition (2). Indeed, it is just sufficient to note in the proof of Theorem 1 that the maps described in (26) are continuous. Hence, if we find the point in $\mathbb{R}^{(m-1)N}$ corresponding to $\mathcal{A}$, approximate it by rational coordinates and go back into the space of wavelet matrices, then we will get the desired $\mathcal{A}'$ (in a similar manner, Vaidyanathan [8] used the parametrization (8) for the same purposes). Such various approximations for Daubechies wavelet matrices of different genus are explicitly constructed in [1].

B. Cryptography. As said in Remark 1, the factorization (7) much resembles the factorization for ordinary polynomials into linear terms. On the other hand, an efficient way of construction of paraunitary matrix polynomials associated to the given points in $\mathbb{F}^{(m-1)N}$ expressed by the diagram (26), which helps to handle such matrix polynomials easily, can be compared to natural parametrization of ordinary polynomials by to their coefficients. An application of polynomial factorization theory in the cryptography is widely known. Having the above similarities (and the advantages mentioned in Remark 1), one can also expect certain applications of the developed theory in the cryptography.

C. Selection of best wavelet matrices. Which wavelet matrix is most suitable to apply in a given practical situation represents frequently a certain optimization problem (which is sometimes very hard to solve) or should be obtained empirically by computer simulations. Having a quick access to the complete bank of compact wavelet matrices due to the parametrization (26) gives an opportunity to choose the best possible wavelet matrix by nearly complete screening.

<div align="center">REFERENCES</div>

[1] L. Ephremidze, A. Gamkrelidze, and E. Lagvilava, "An approximation of Daubechies wavelet matrices by perfect reconstruction filter banks with rational coefficients", (to appear in *Adv. Comput. Math.*).

[2] L. Ephremidze, G. Janashia and E. Lagvilava, "On the factorization of unitary matrix-functions", *Proc. A. Razmadze Math. Inst.*, vol. 116, pp. 101–106, 1998.

[3] ———, "A simple proof of matrix-valued Fejér-Riesz theorem", *J. Fourier Anal. Appl.*, vol. 15, no. 1, pp. 124–127, 2009, (DOI: 10.1007/s00041-008-9051-z).

[4] ———, "On approximate spectral factorization of matrix functions", to be published in *J. Fourier Anal. Appl.*, (DOI: 10.1007/s00041-010-9167-9).

[5] G. Janashia, E. Lagvilava, and L. Ephremidze "A new method of matrix spectral factorization", *IEEE Trans. Inform. Theory*, vol. 57, no. 4, pp. 2318–2326, 2011, (DOI: 10.1109/TIT.2011.2112233).

[6] J. Kautsky and R. Turcajova, "Pollen product factorization and construction of higher multiplicity wavelets", *Lin. Algebra Appl.*, vol. 222, pp. 241–260, 1995.

[7] H. L. Resnikoff and R. O. Wells, *Wavelet Analysis*, Springer-Verlag, 1998.

[8] P. P. Vaidyanathan, *Multirate Systems and Filter Banks*, Prentice Hall, New Jersey, 1993.

Authors' Addresses:

L. Ephremidze, E. Lagvilava
A. Razmadze mathematical Institute
I. Javakhishvili State University
2, University Street, Tbilisi 0143, Georgia
E-mails: *lephremi@umd.edu; edem@rmi.ge*